Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description

06/06/2019	1.0	M. Elbanhawi	First submission

Table of Contents

Purpose of the Functional Safety Concept

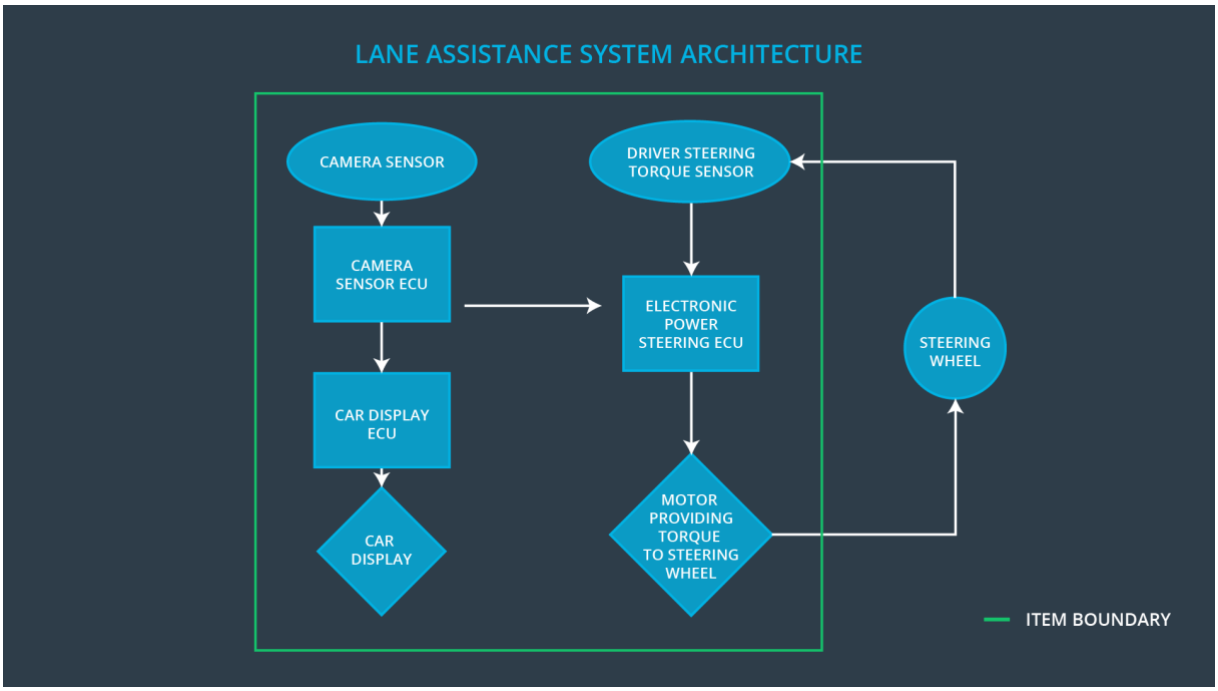
The purpose of the functional safety document is to allocate functional requirements and their attributes based on the safety goals defined in the hazard and risk assessment.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The LDW function shall be torque limited to avoid oscillations and loss of control.
Safety_Goal_02	The LKA function shall be time limited and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system as an autonomous driving feature.
Safety_Goal_03	The LDW function shall not be active in case of a camera subsystem malfunction
Safety_Goal_04	The LKA function shall not be active in case of a camera subsystem malfunction

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Responsible for capturing images sending them to the camera ECU.
Camera Sensor ECU	Responsible for processing image, detecting lanes and the position of the vehicle within the lane.
Car Display	Human machine interface for alert and warnings to the driver.
Car Display ECU	Responsible for controlling the display component to indicate the statues of LDW and LKA functions.
Driver Steering Torque Sensor	Measure input torque by the driver
Electronic Power Steering ECU	Apply a necessary torque to the steering wheel based on a command from LDA and LKD systems.
Motor	Applies torque requested by ECU

Functional Safety Concept

The functional safety concept consists of:

- Functional safety analysis
- Functional safety requirements
- Functional safety architecture
- Warning and degradation concept

Functional Safety Analysis

Malfunction ID	**Main Function of the Item Related to Safety Goal Violations**	**Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)**	**Resulting Malfunction**
Malfunction_01	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	LDW apply a high torque on a slippery wet road at high speed driving
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	LDW apply a high torque on a slippery wet road at high speed driving
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	LKA is active and the driver is not required to keep hands on steering wheel. Results in misuse of LKW as Autonomous driving mode.

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Disable system
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency		50 ms	Disable system

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 01-01	Apply an oscillating torque amplitude is below Max_Torque_Amplitude and validate the drive does not lose control of the vehicle and is aware of the warning	Verity the system is disabled if torque amplitude is above Max_Torque_Amplitude
Functional Safety Requirement 01-02	Apply an oscillating torque frequency is below Max_Torque_Frequency and validate the drive does not lose control of the vehicle and is aware of the warning	Verity the system is disabled if frequency is below Max_Torque_Frequency

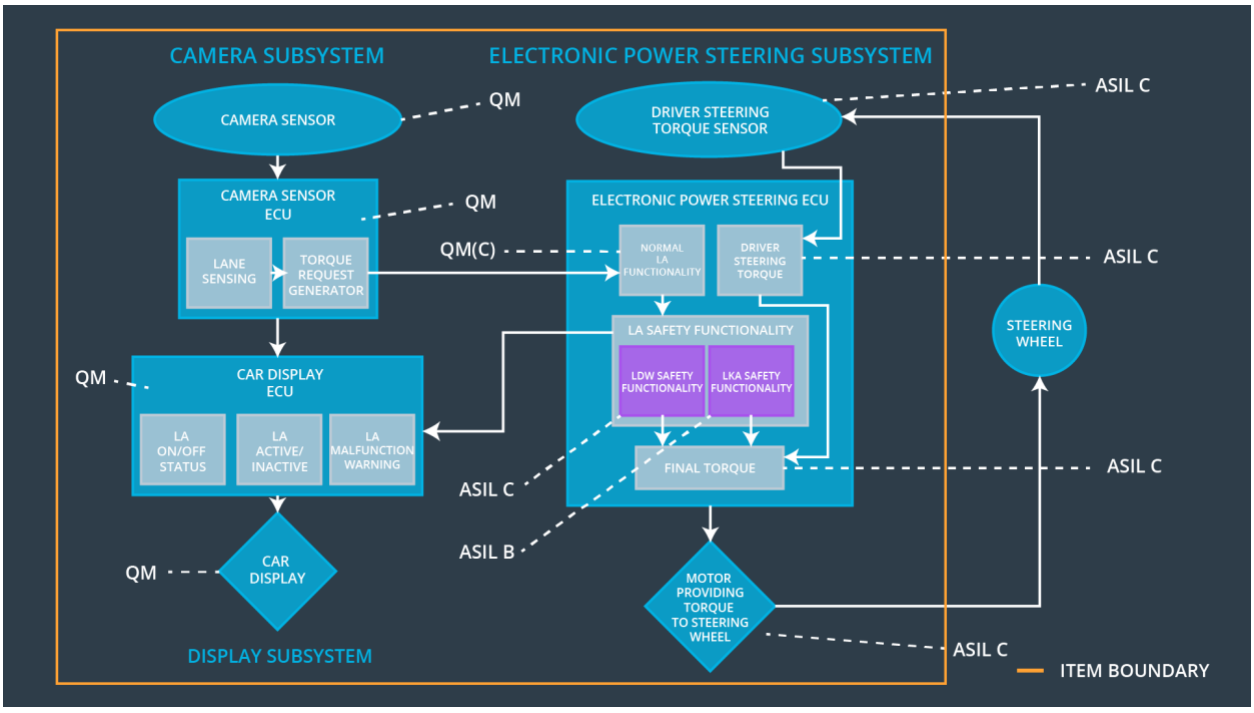
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall limit lane keeping assistance torque for only Max_Duration	B	500 ms	Disable system.

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-01	Test the Max_Duration of 500ms and validate that drivers maintain their hands on the wheel and do not abuse the system.	Verify that the system is disabled after exceeding Max_Duration

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	Apply an oscillating torque amplitude is below Max_Torque_Amplitude and validate the drive does not lose control of the vehicle and is aware of the warning	**X**		
Functional Safety Requirement 01-02	Apply an oscillating torque frequency is below Max_Torque_Frequency and validate the drive does not lose control of the vehicle and is aware of the warning	**X**		
Functional Safety Requirement 02-01	The electronic power steering ECU shall limit lane keeping assistance torque for only Max_Duration	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Disable LDW system	Malfunction_01 Malfunction_02	Yes	Dashboard alert
WDC-02	Disable LKA system	Malfunction_03	Yes	Dashboard alert